

1 / 17

FIG.2

SUBSTITUTION TABLE

8	1	3	F
A	6	C	5
4	9	0	E
B	2	7	D

FIG.1B

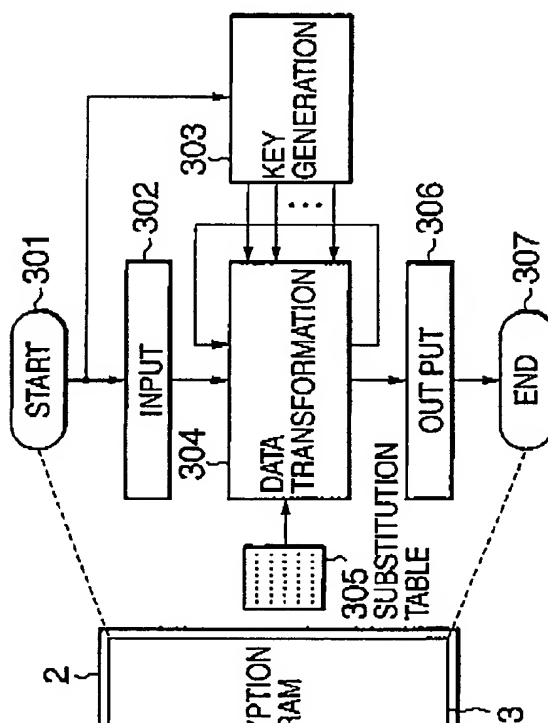
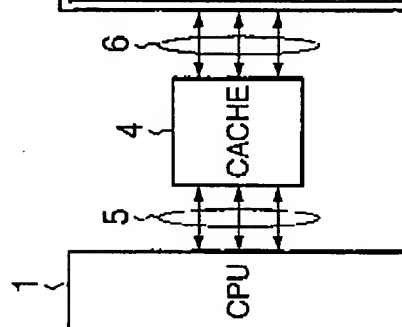


FIG.1A

(PRIOR ART)



2 / 17

FIG.3

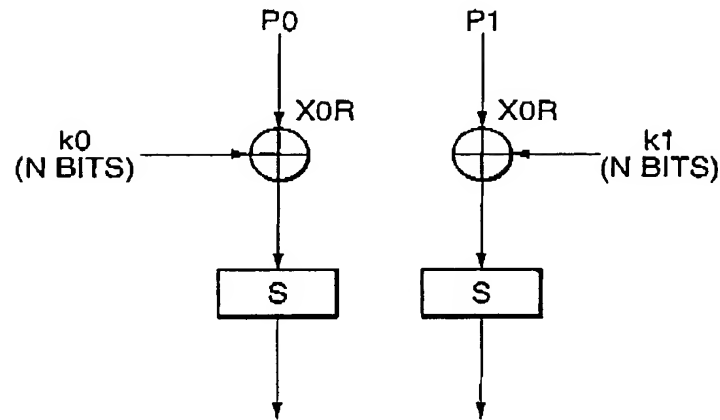


FIG.4A

Δk	
00	0
01	0
02	0
03	0
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
ff	0

$\Delta k \neq P_i \oplus P_j$

FIG.4B

Δk	
00	15
01	16
02	17
03	0
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
ff	20

- DETERMINED KEY DIFFERENTIAL $\Delta k \neq P_i \oplus P_j$

3 / 17

FIG.5A

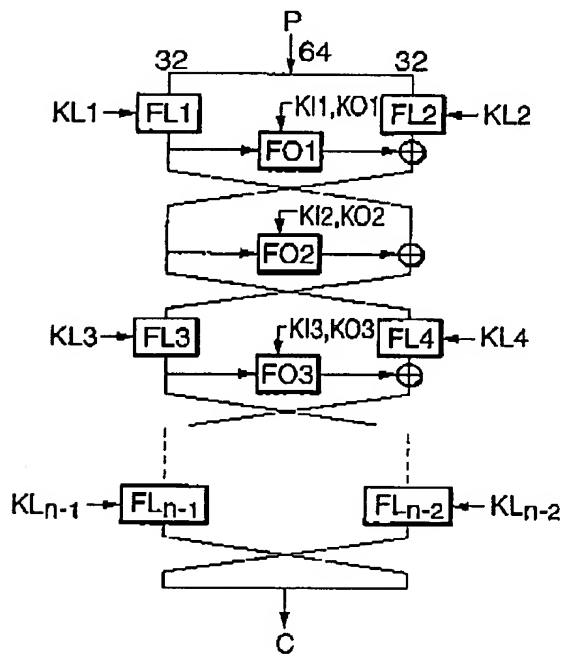


FIG.5B

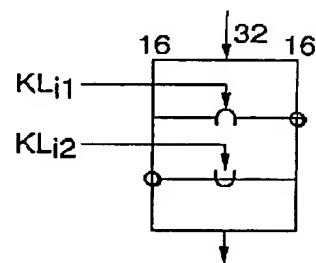
FUNCTION FL_i 

FIG.5C

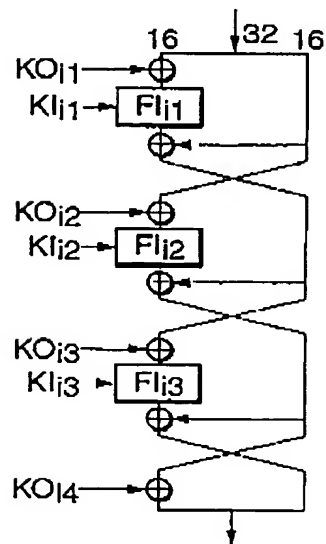
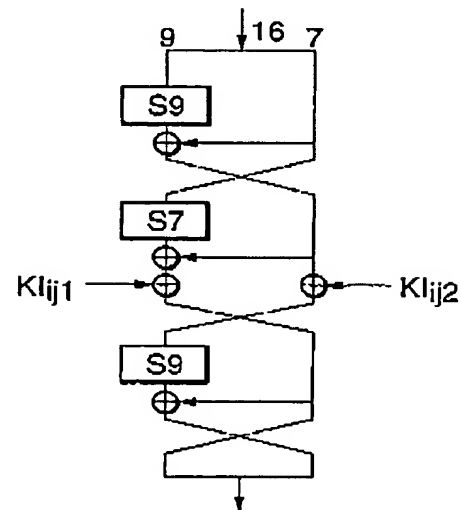
FUNCTION FO_i 

FIG.5D

FUNCTION Fl_{ij} 

4 / 17

FIG.6

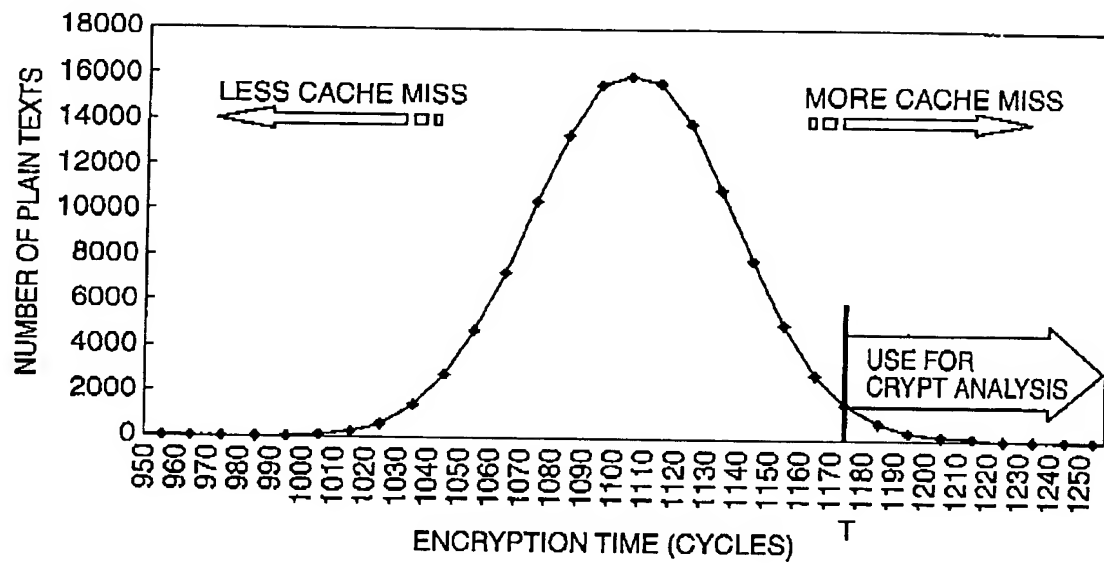
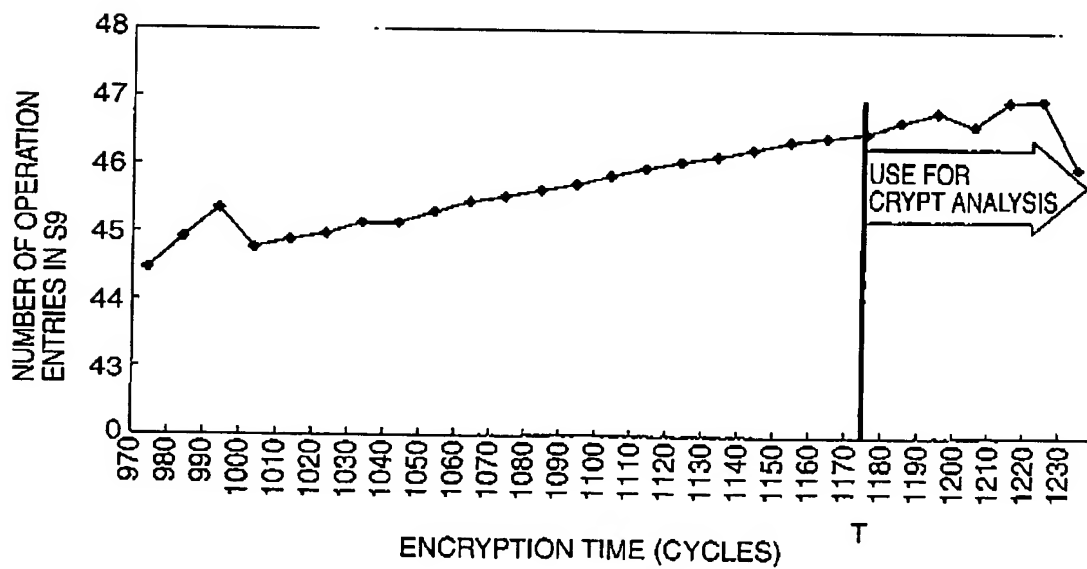
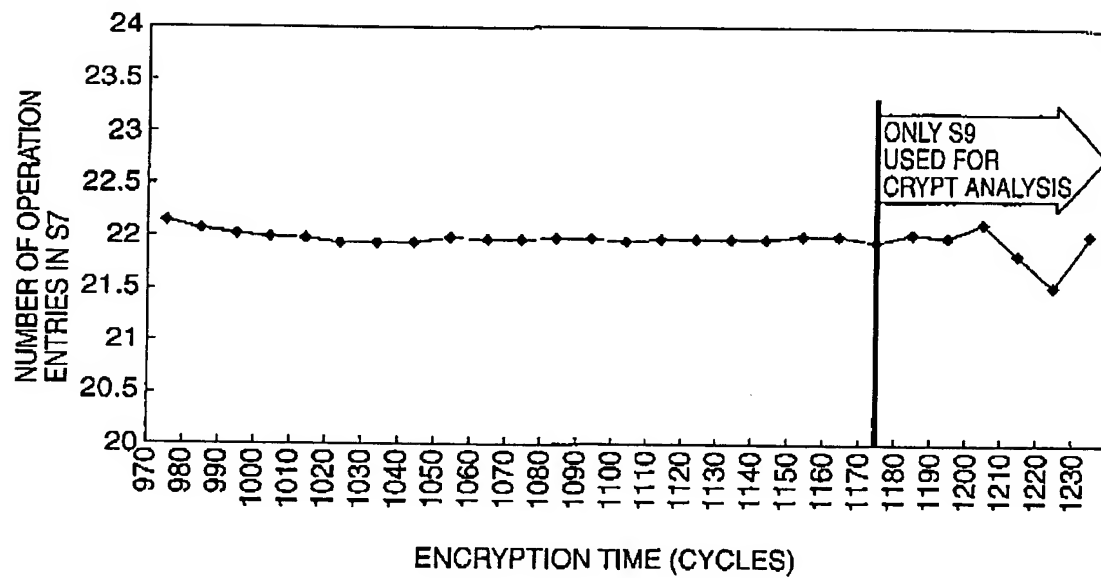


FIG.7



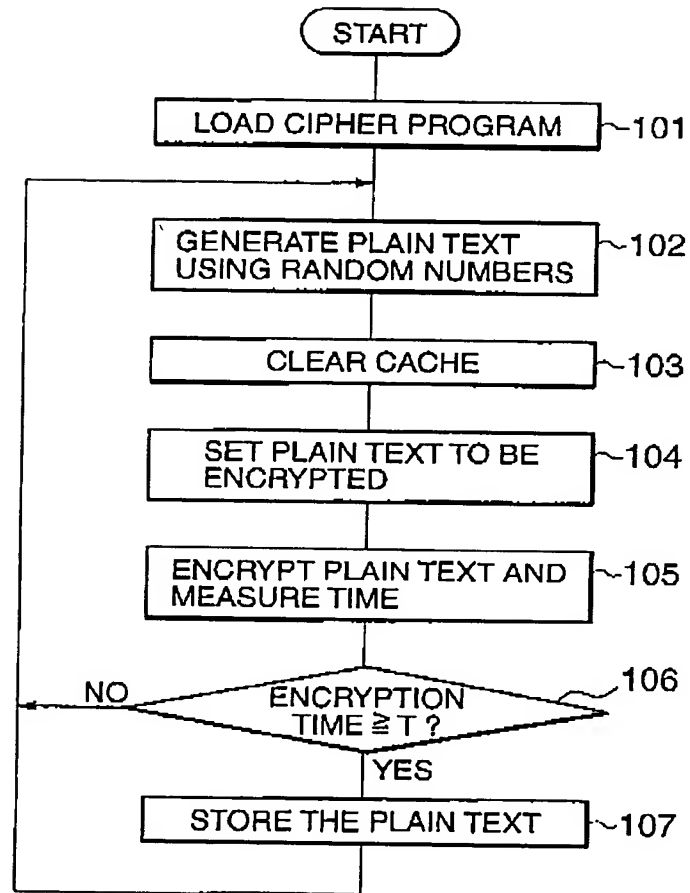
5 / 17

FIG.8

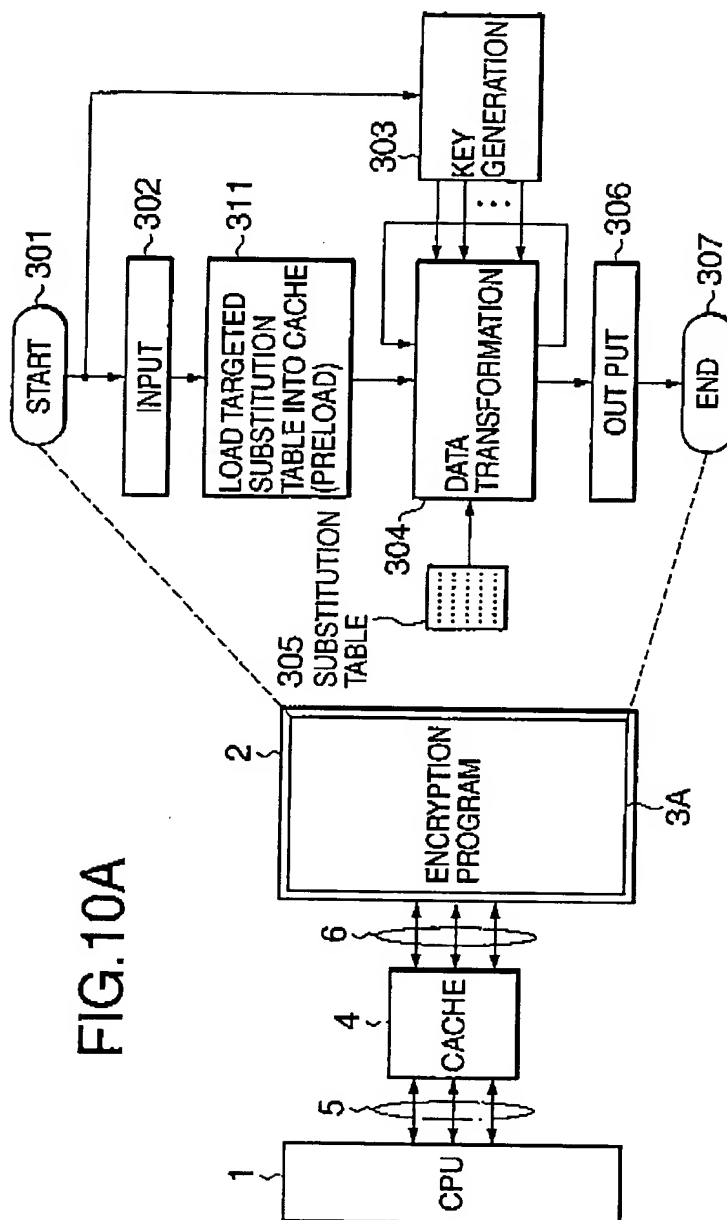


6 / 17

FIG.9



7 / 17

FIG. 10B
(INVENTION)

8 / 17

FIG.11B

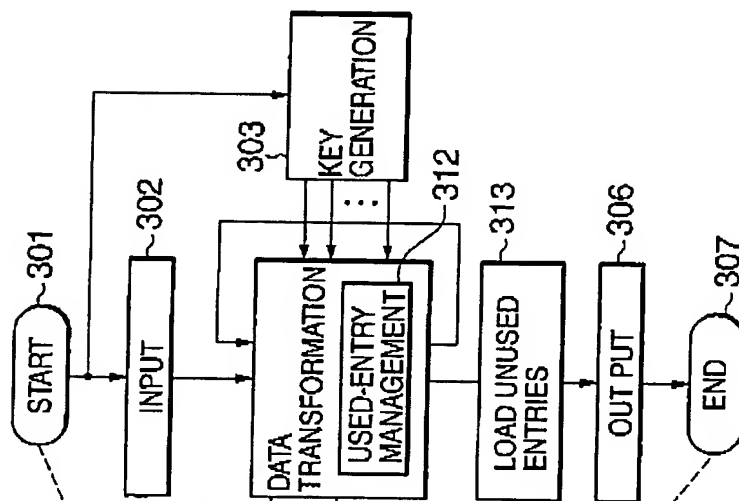


FIG.11A

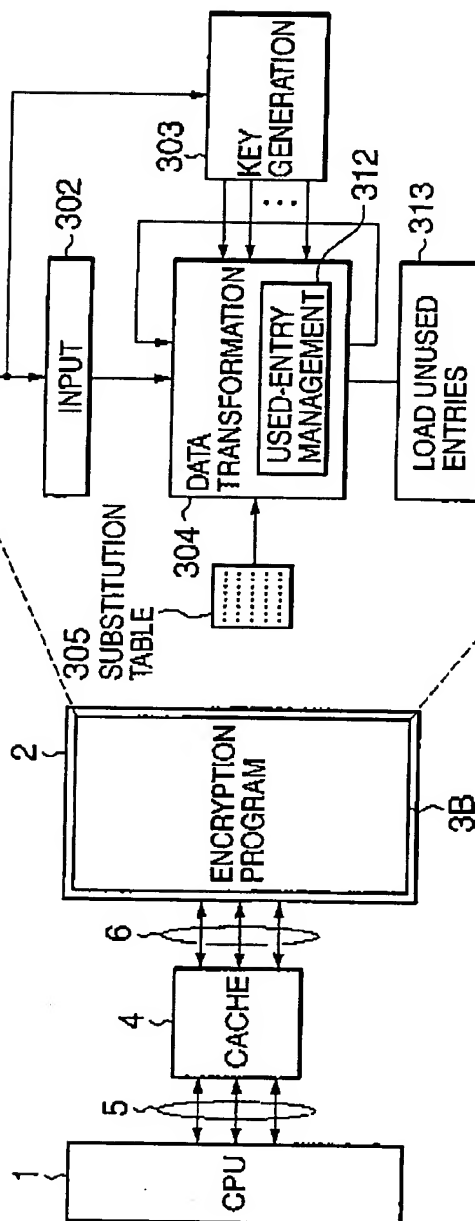


FIG.11C

X	O	X	...
O	X	X	...
X	O	O	...
:	:	:	:

9 / 17

FIG. 12B

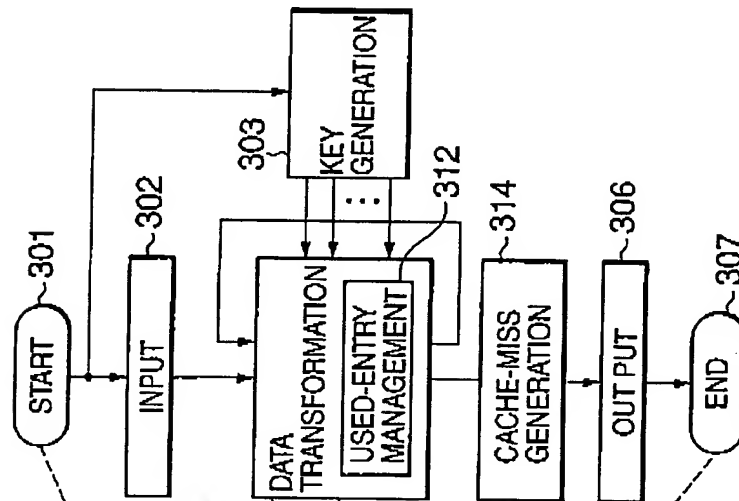
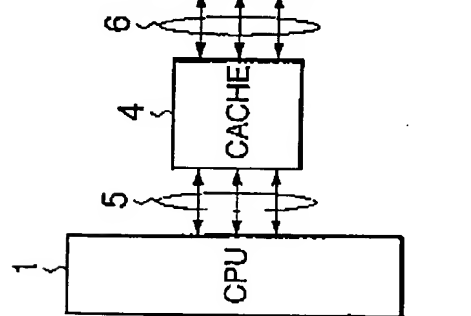


FIG. 12A



10 / 17

FIG.13B

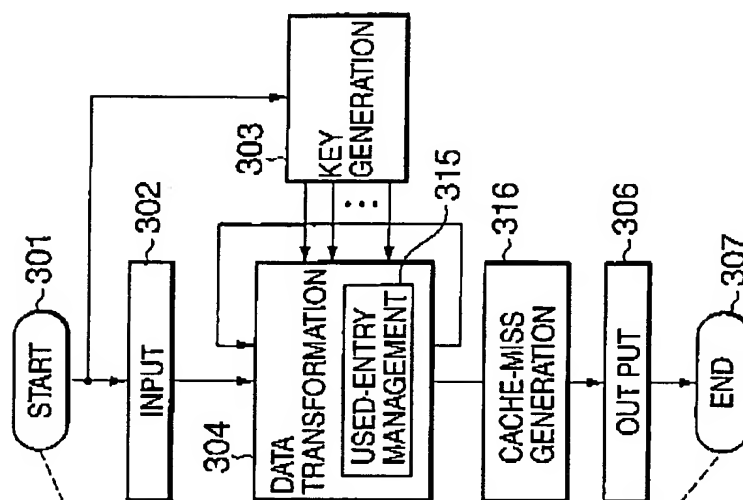


FIG.13A

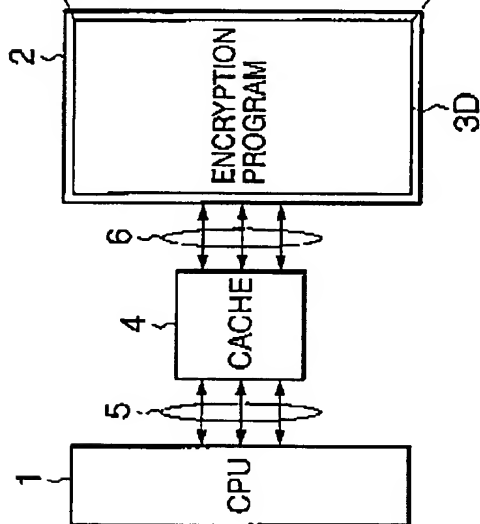


FIG.13C

0	2	0	...
1	0	0	...
0	1	2	...
:	:	:	:

11 / 17

FIG.14B

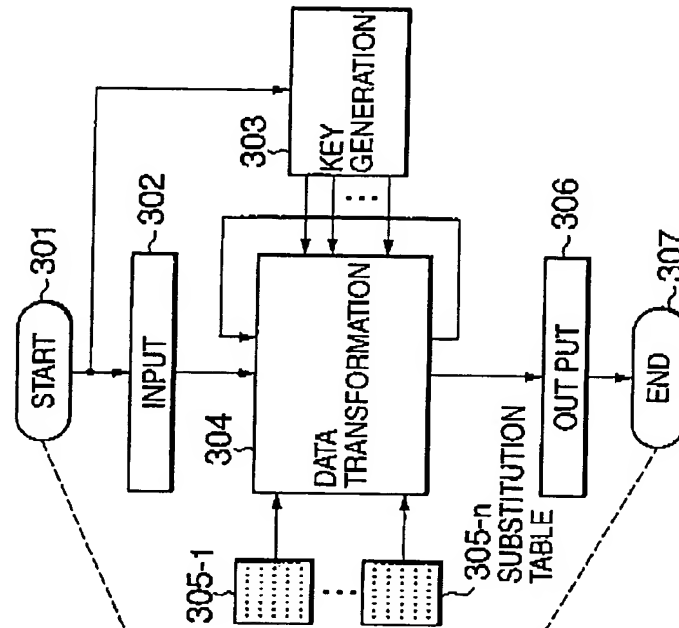
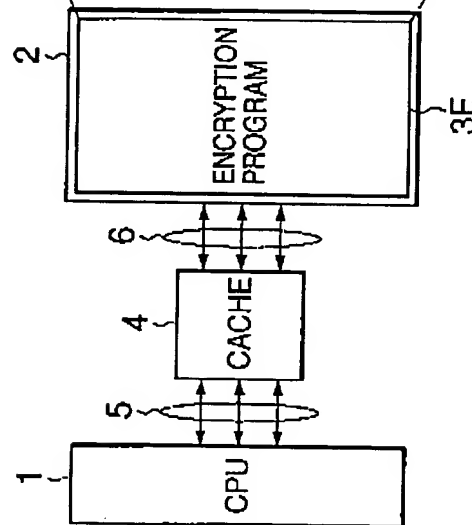


FIG.14A



12 / 17

FIG.15B

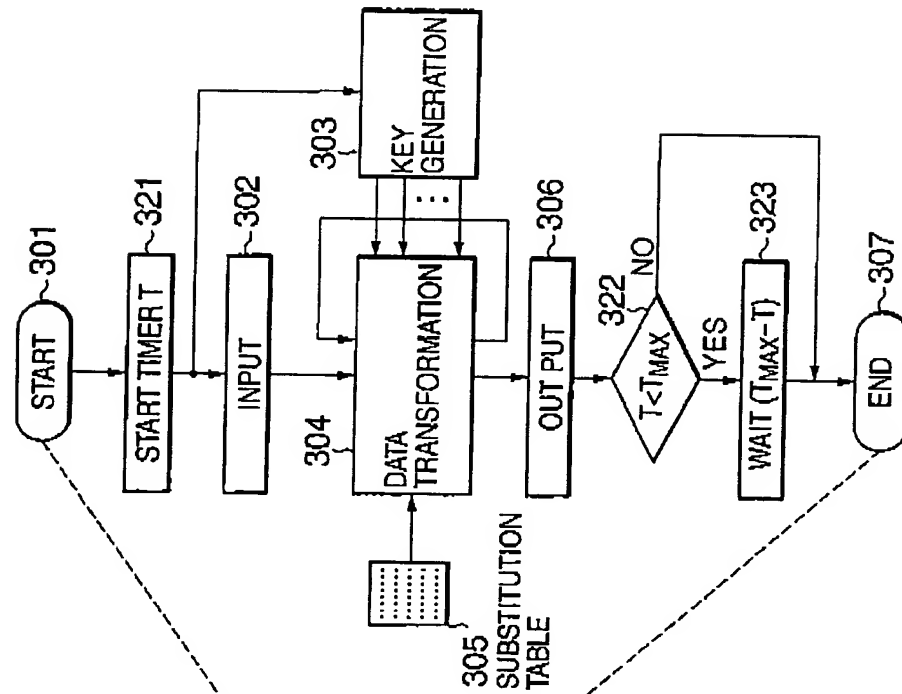
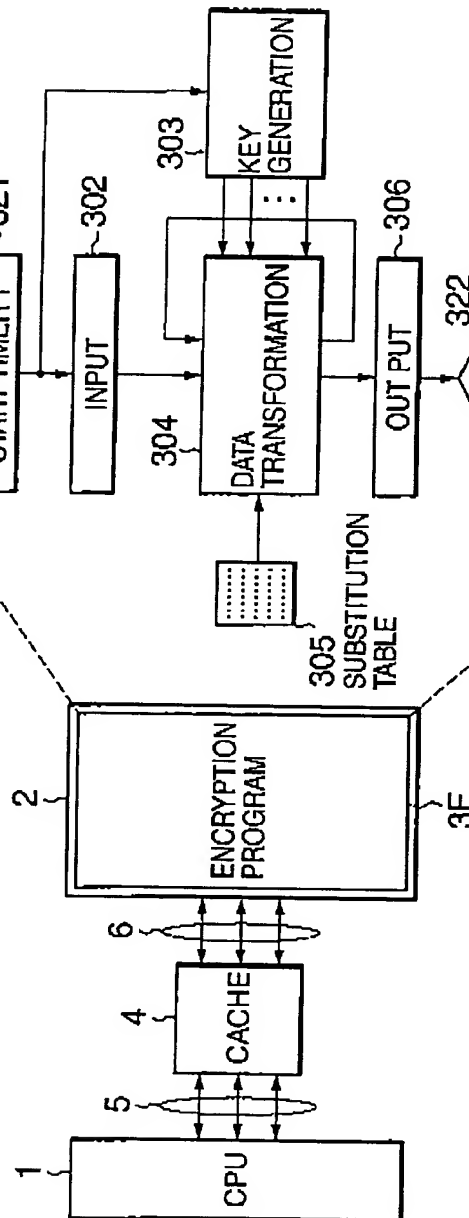


FIG.15A



13 / 17

FIG.16B

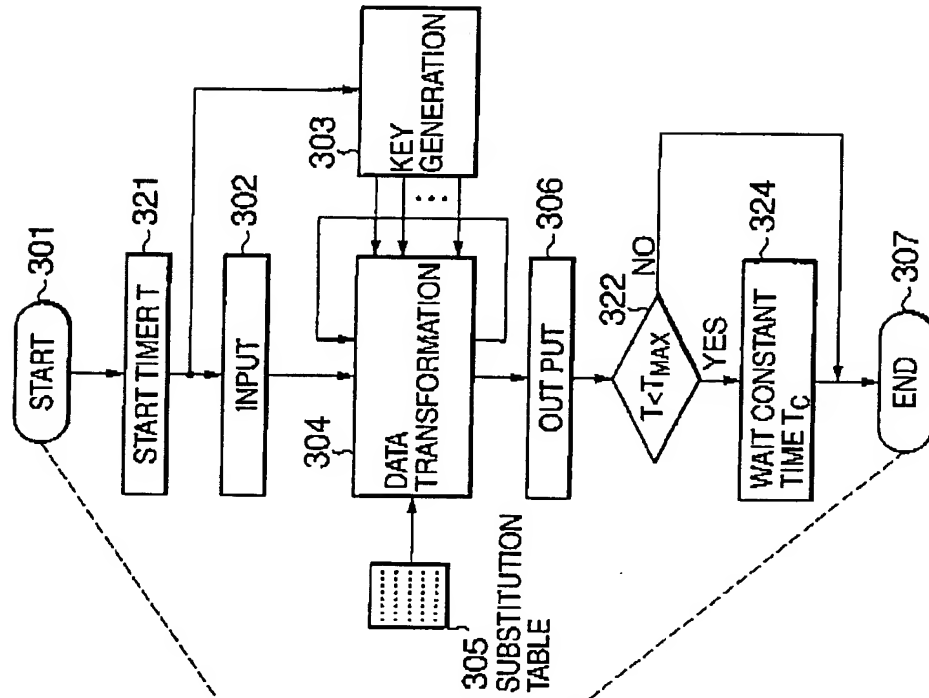
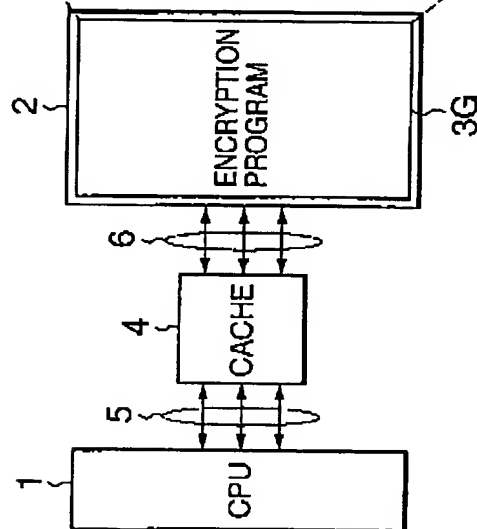
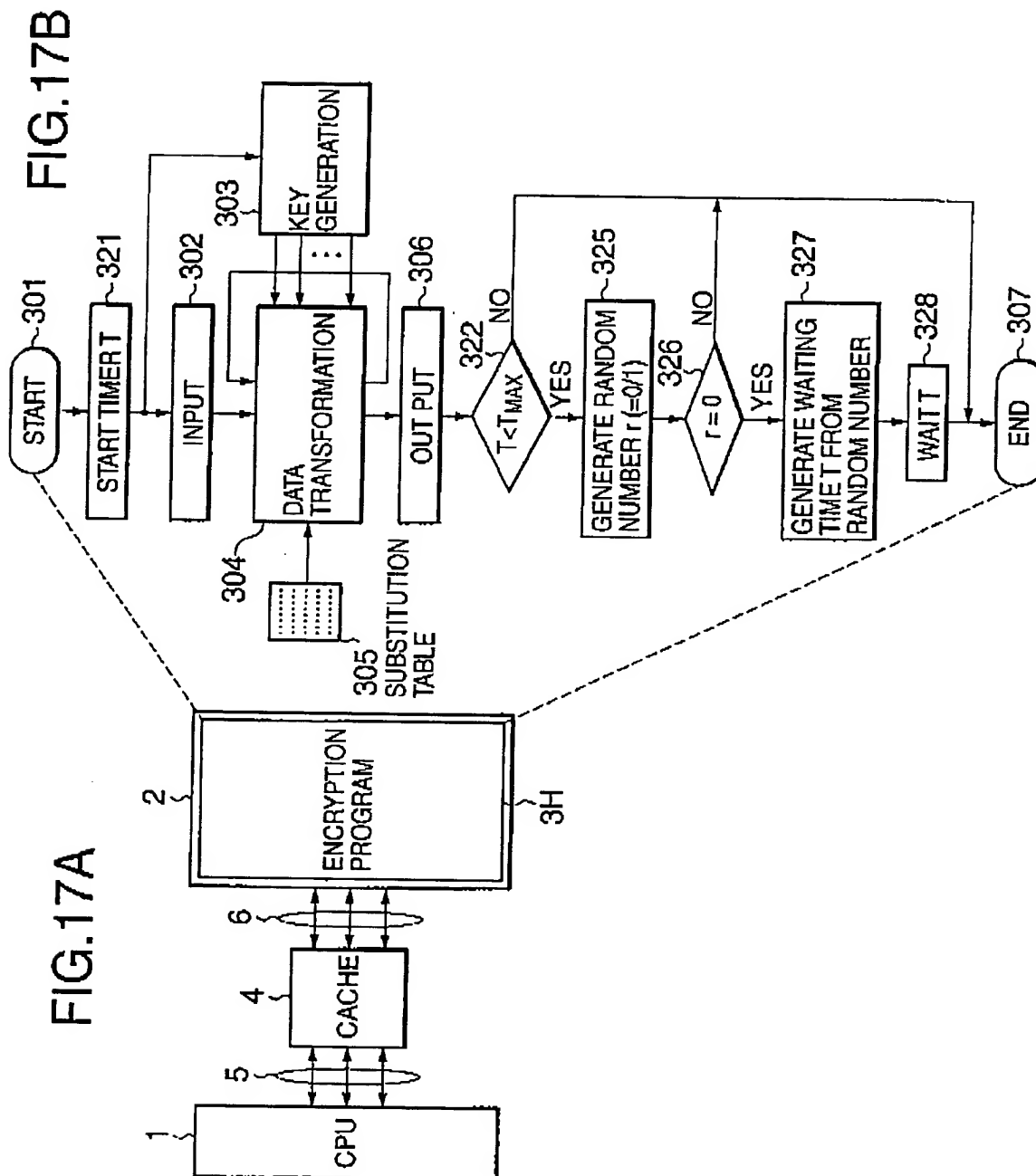


FIG.16A



14 / 17



15 / 17

FIG.18B

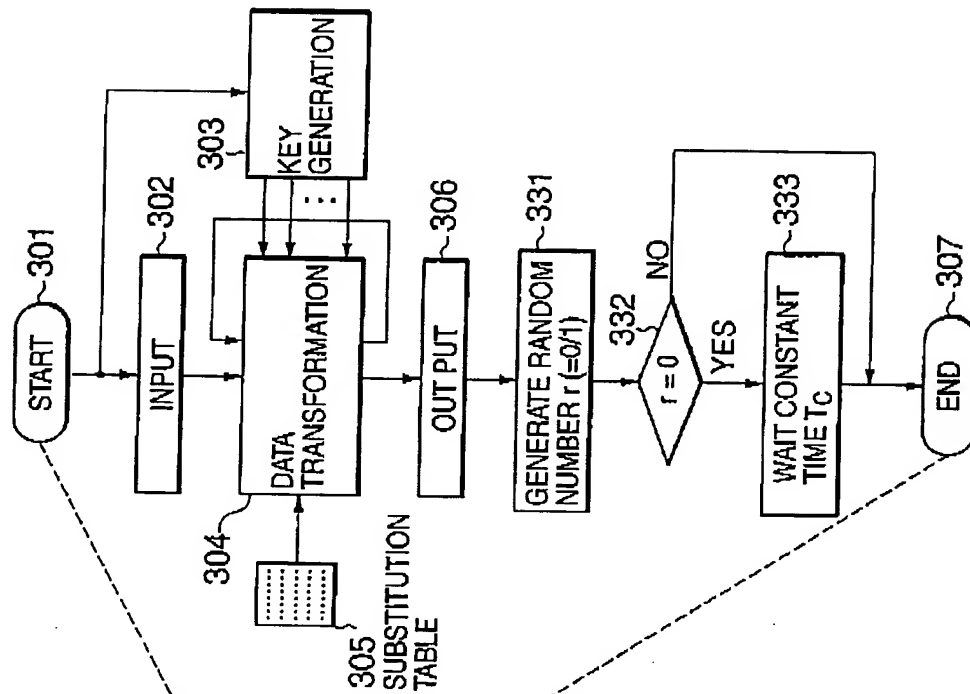
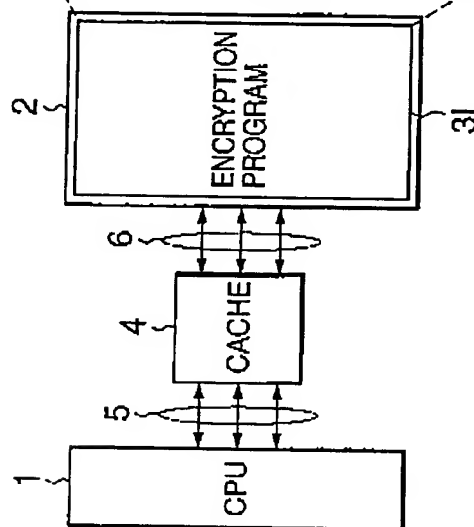


FIG.18A



16 / 17

FIG. 19B

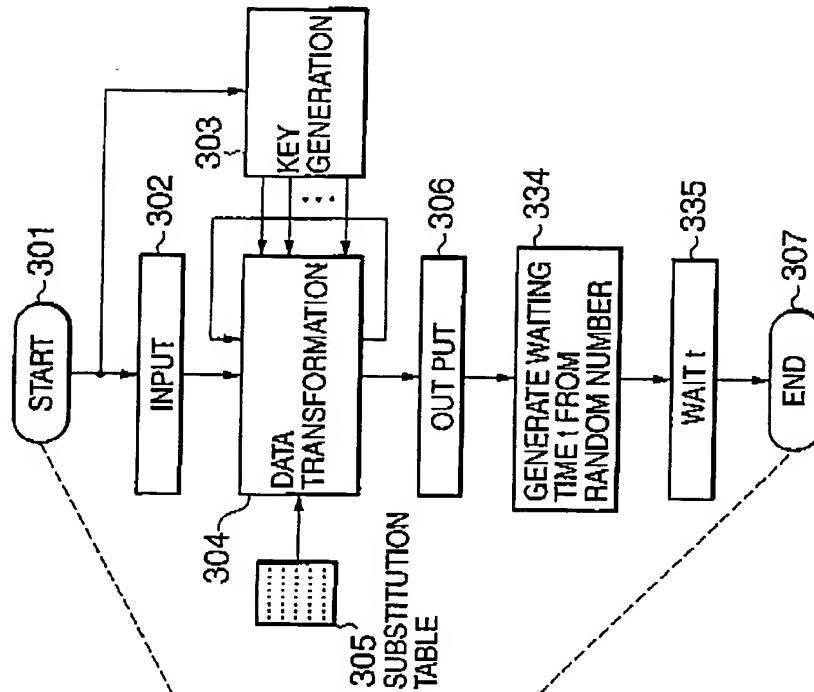
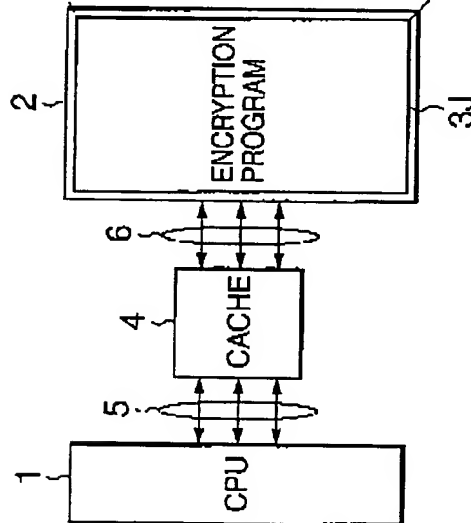


FIG. 19A



17 / 17

